Assignment 4

Courtney Hagen

W0263284

OSYS3030

Table of Contents

[Introduction 3](#_Toc23013685)

[Change Management Log 3](#_Toc23013686)

[OSYS3030-LX01 3](#_Toc23013687)

[OSYS3030-LX02 4](#_Toc23013688)

[Questions 5](#_Toc23013689)

[Question 1 5](#_Toc23013690)

[Question 2 5](#_Toc23013691)

[Question 3 5](#_Toc23013692)

[Question 4 5](#_Toc23013693)

[Question 5 5](#_Toc23013694)

[Question 6 5](#_Toc23013695)

[Question 7 5](#_Toc23013696)

[Question 8 5](#_Toc23013697)

[Screenshots 5](#_Toc23013698)

[References 8](#_Toc23013699)

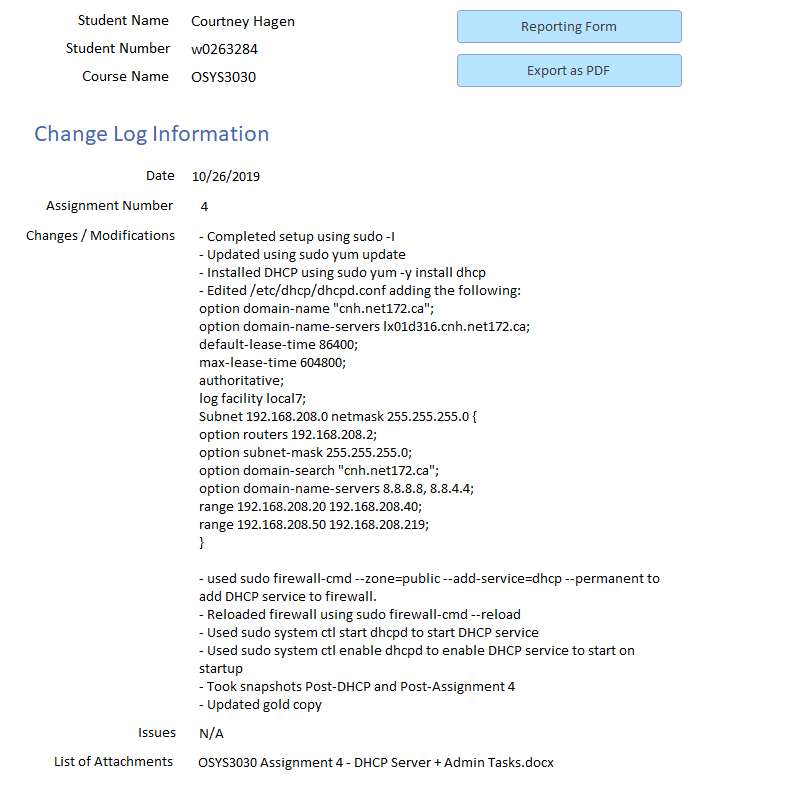
Assignment 4

# Introduction

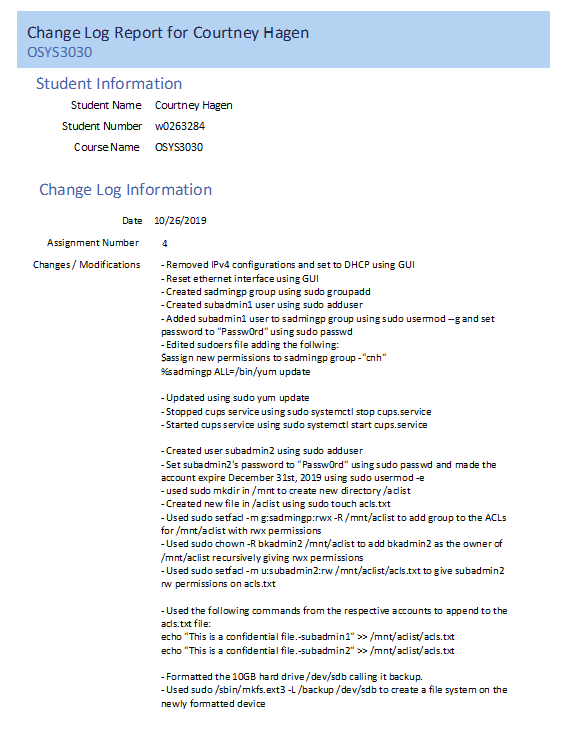
The purpose of this assignment is to demonstrate using DHCP with CentOS as well as administrating ACLs.

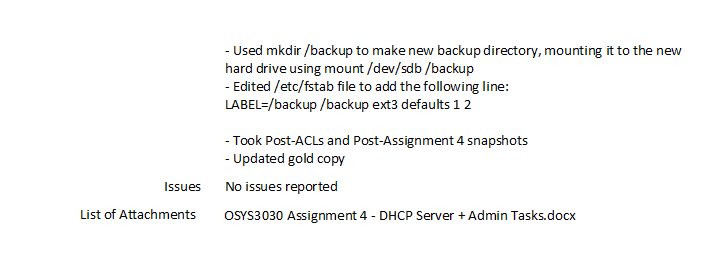
# Change Management Log

## OSYS3030-LX01



## OSYS3030-LX02





# Questions

## Question 1

The active state of the cups service is “loaded active running”, meaning that not only is it loaded and actively working, but its’ processes are running in the background.

## Question 2

When stopping the cups service, a warning stating that cups can still be activated by cups.socket and cups.path appears.

## Question 3

The active status of the cups service after being stopped is “loaded active waiting” under the cups.path service, meaning the cups service is waiting on cups.path to run the cups service again.

## Question 4

Cups.service is loaded from /usr/sbin/cupsd.

## Question 5

ACL’s are Access Control Lists and in Linux, like other operating systems, their purpose is to set permissions for access.

## Question 6

Default ACLs are used as the permissions a folder, subfolder, or files use when no other specification is made. That is, for example, a default ACL can be set that the creator of a directory has permissions to all subdirectories. An Access ACL can be used to disrupt this, by adding extra ACLs like permissions for another user, or removing certain permissions on a certain file. (Access Control Lists in Linux, 2003)

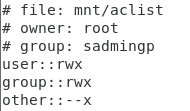
## Question 7

ACLs that use three entries are minimal ACLs. The entries they use are ‘r’,’w’, and ‘x’. Any ACLs that use more than this are extended ACLs. Both can be used on directories, subdirectories, and files. Extended ACLs give more control over applying specific permissions. (Grünbacher, 2003)

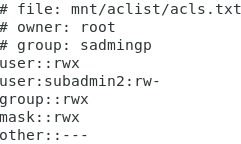
## Question 8

When used with the setfacl command, -m is used to modify already existing ACLs.

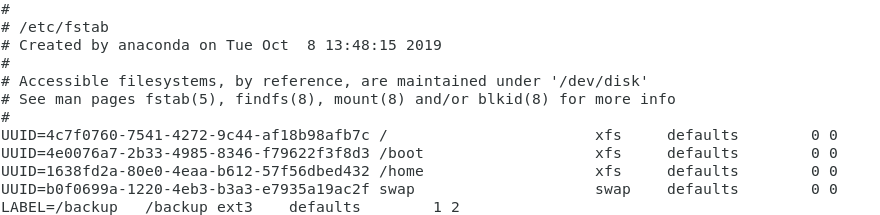
# Screenshots



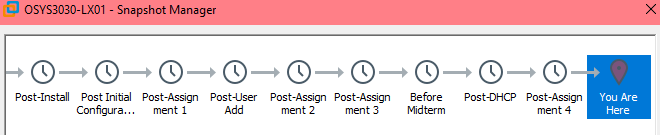
This screenshot shows the results of the getfacl command on /mnt/aclist.



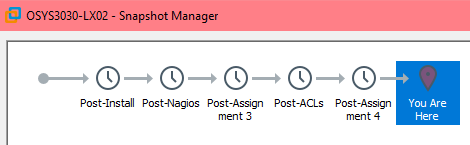
This is the result of the getfacl command on /mnt/aclist/acls.txt



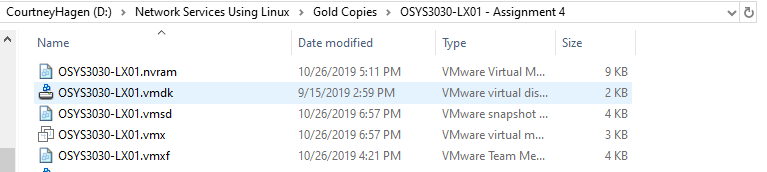
This screenshot shows the modifications made to the /etc/stab file.



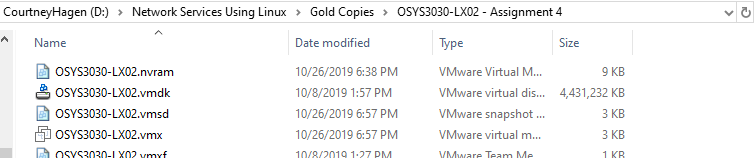
This screenshots demonstrates the post-assignment snapshot of OSYS3030-LX01



This shows the post-assignment snapshot of OSYS3030-LX02.



This shows that I have created an Assignment 4 Gold Copy of OSYS3030-LX01.



This demonstrates my Assignment 4 Gold Copy of OSYS3030-LX02.

# References

Access Control Lists in Linux. (2003, May 11). Retrieved October 26, 2019, from <http://www-uxsup.csx.cam.ac.uk/pub/doc/suse/suse9.0/adminguide-9.0/node27.html#SECTION06234000000000000000>.

Grünbacher, A. (2003, April 4). POSIX Access Control Lists on Linux. Retrieved October 26, 2019, from https://www.usenix.org/legacy/publications/library/proceedings/usenix03/tech/freenix03/full\_papers/gruenbacher/gruenbacher\_html/main.html.